219836-1

DISCUSSION DRAFT
MARCH 25, 1998

MODEL CERTIFICATE POLICY

Government Information Technology Services
Federal PKI Task Force
Business and Legal Work Group

Prepared for the Federal PKI Task Force by:

Thomas J. Smedinghoff
McBride Baker & Coles
500 W. Madison Street, 40th Floor
Chicago, Illinois 60661
(312) 715-5700
www.mbc.com
smedinghoff@mbc.com

March 25, 1998 Draft

TABLE OF CONTENTS

I. INTRODUCTION

This Model Certificate Policy is presented as a guide for relying parties in both the public and private sectors in establishing and/or reviewing certificate policies suitable for transactions they will be entering into. This introduction sets forth the nature, purpose, and role of a certificate policy.

A. What is a Certificate Policy?

Government and private entities that accept electronic communications need assurance that the digitally signed messages they receive can be verified with reference to a certificate that is appropriately trustworthy for the intended purpose. There is an increasing recognition that this assurance can be provided through the use of a *certificate policy*. This section defines the concept of a certificate policy, and clarifies its role in digitally signed communications.

The term *certificate policy* comes from the X.509 version 3 certificate specification, where it is defined as follows:

> *certificate policy*: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.[1]

Unfortunately, the X.509 specification does not include any further discussion of the concept of a certificate policy, and does not state what a certificate policy should contain. We do know that the X.509 certificate policy concept is an outgrowth of the "policy statement" concept developed for Internet privacy enhanced mail,[2] but it has never been clearly articulated in the literature, and any discussion of it has usually been brief and cryptic.

The X.509 definition implies that a certificate policy is intended only to state (or limit) the uses that are authorized for a given certificate (e.g., that a certificate may be used for "the authentication of electronic data interchange transactions for the trading of goods within a given price range"). However, other more informal discussions of a certificate policy describe it as a statement of the "strength" of a certificate, based on the mechanisms used for the generation, management and revocation of the certificate. Thus, it is often described as a statement used by a

[1] ITU-T X.509 Recommendation, Section 3.3.

[2] See, Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework," PKIX Working Group Internet Draft, September 30, 1997, Section 1.1; S. Kent "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management," Internet RFC 1422, § 3.4 (February, 1993); and Michael S. Baum, "Federal Certification Authority Liability and Policy," NIST-GCR-94-654, pp 347-360 (June 1994).

relying party "to determine the degree of assurance of trust which can be placed in the authenticity and integrity of the public keys contained in certificates issued by the certification authority."[3]

Understanding the concept of a certificate policy also requires consideration of the related concept of a *certification practice statement*, which was first articulated in the American Bar Association Digital Signature Guidelines.[4] A certification practice statement ("CPS") is defined as "a statement of the practices which a certification authority employs in issuing the certificates."[5] The term was chosen, in part, "to avoid ambiguity or confusion in the usage of the word 'policy'."[6]

Unfortunately, this has created additional confusion, as it is often unclear whether a certificate policy and a CPS are the same thing or two different things. In some cases, the same document is treated as both a certificate policy and a certification practice statement.[7] In other cases, a CPS is viewed simply as "a more detailed description of the practices followed by a CA in issuing and otherwise managing certificates.[8] Thus, some commentators specify the same list of topics for inclusion in both a certificate policy and a CPS.[9] Quite clearly, "the precise relationship between a CPS and an X.509 certificate policy definition is neither crystal clear nor universally agreed-upon."[10] This suggests, of course, that the difference between a certificate policy and a certification practice statement lies not in the topics covered, but rather in the focus or perspective from which those topics are covered.

---

[3] See, e.g., Sharon Boeyen, "Certificate Policies and Certification Practice Statements," February 1997 (Entrust Technologies White Paper, Version 1.0), Section 1.

[4] Information Security Committee, Electronic Commerce Division, Section of Science and Technology, American Bar Association, ABA Digital Signature Guidelines, § 1.8 (August, 1996). The ABA Digital Signature Guidelines are available at *www.abanet.org*/ec/isc/*dsgfree.html*. Like the certificate policy concept, the CPS concept is also "rooted in the concepts of *Policy Certification Authorities* (PCAs) and their *policy statements* that were introduced in the Internet Privacy Enhanced Mail (PEM) design . . . described in Internet RFC 1422." Warwick Ford and Michael S. Baum, Secure Electronic Commerce, (1997) at p. 360.

[5] ABA Digital Signature Guidelines Section 1.8 "Certification Practice Statement"

[6] ABA Digital Signature Guidelines Section 1.8 "Certification Practice Statement", Related Terms.

[7] Warwick Ford and Michael S. Baum, Secure Electronic Commerce, (1997) at p. 362. In fact, the Verisign, Inc. Certification Practice Statement states that "this CPS constitutes a 'certificate policy' as defined by X.509 Amendment 1 to ISO/IEC 9594-9: 1995." Verisign CPS, version 1.2, May 30, 1997.

[8] Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997, at Section 1.1. (See also, section 3.6, which notes that CPSs "will generally be more detailed than certificate policy definitions").

[9] See, Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997, at Section 4; and Sharon Boeyen, "Certificate Policies and Certification Practice Statements," February 1997 (Entrust Technologies White Paper, Version 1.0), Section 3.

[10] Warwick Ford and Michael S. Baum, Secure Electronic Commerce, (1997) at p. 361.

This Model Certificate Policy rejects the view that a certificate policy and a CPS are the same thing, or that one is simply a more detailed description of the same topics covered by the other. Instead, it is based on the view that a certificate policy that fulfills a purpose separate from a CPS. Specifically, a certificate policy (and the difference between a certificate policy and a CPS) is defined primarily in terms of (1) authorship, (2) purpose, (3) level of specificity, and (4) approach.

1. Authorship

The author of a certificate policy and the author of a CPS are not normally the same. A CPS is typically prepared by a certification authority,[11] with "a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.[12] A certificate policy, on the other hand, "may be defined by *any* organization with a need."[13] As such, it "represents a limited set of practice provisions that can be commonly agreed-upon and understood by a community of organizations," and that can constitute a basis for immediately accepting certificates in a useful set of locally approved application scenarios.[14]

Thus, unlike a CPS, a certificate policy is normally *not* prepared by a CA. Rather, it is more likely defined by any number of *relying party* entities, including:

- a single relying party (e.g., a government agency or other large entity that contemplates significant electronic transactions) seeking to define the criteria that must be agreed to and complied with by a CA before certificates issued by such CA will be accepted by such relying party

- an industry association or other group of entities seeking to define their commonly held belief with regard to the level of trust that must be met by certificates used for particular purposes.[15]

---

[11] "A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate . . . . ABA Digital Signature Guidelines Section 1.8.1. However, the ABA Digital Signature Guidelines recognize that a CPS may also be "a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber." ABA Digital Signature Guidelines Section 1.8.1

[12] Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997 at Section 3.6.

[13] ITU-T X.509 Recommendation, Section 12.2.2.5 (emphasis added).

[14] Warwick Ford and Michael S. Baum, Secure Electronic Commerce (1977) at page 362.

[15] "At some time in the future, industry forums are expected to establish standard certificate policies for their respective business sectors. At such time, a policy authority may simply adopt or adapt a model certificate policy from such an association. In the meantime, the policy authority must develop a certificate policy on its own." Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 2.

In either case, persons who wish to communicate digitally signed messages with entities specifying a particular certificate policy requirement will have to obtain a certificate from a CA that adopts such certificate policy and references it in the certificates it issues.

CAs whose certificates meet the qualifications of a particular certificate policy might then represent, warrant, or certify (i.e., "assert") that a specific class or type of their certificates meet the requirements of the certificate policy.[16] This might be done, for example, by including a reference to the policy in the "*certificatePolicies*" public key certificate extension in an X.509 version 3 certificate.[17]

Thus, each certification authority in an open system environment would publish a CPS governing the certificates that it issues and specifying the details of the practices that it employs issuing those certificates. In addition, however, each certification authority might also adopt one or more certificate policies issued by third parties as, in effect, a representation that its certificates are issued in accordance with the requirements of those policies.

For example, the federal government might define a government-wide certificate policy for handling confidential human resources information. The certificate policy will be a broad statement of the general characteristics of the CA Services required for issuance of certificates suitable for this type of application. Private certification authorities, as well as different government departments or agencies that operate certification authorities, each of which operates under its own certification practice statement, might support this certificate policy. At the same time, such certification authorities may support other certificate policies.[18]

---

[16] How a CA becomes entitled to claim that its certificates meet the requirements of a particular certificate policy may be a major issue for discussion. See Part B below.

[17] Under one approach, the certificate policy is registered with a policy administering organization and assigned a unique "object identifier" (OID). An object identifier is a specially-formatted number, which is registered with an internationally-recognized standards organization. Certification Authorities "assert" that a certificate was generated in accordance with a specific certificate policy by including the relevant policy OID in the "*certificatePolicies*" public key certificate extension in an X.509 version 3 certificate. The *certificatePolicies* field in the X.509 certificate specifies the policies under which the certificate was issued to the user and/or the types of uses applicable to the certificate. It is possible to designate a number of certificate policies within a certificate. If the certificate policy's field is set to be non-critical, the CA indicates which policies apply to the certificate, but is not requiring the certificate to be limited in use to situations only in accordance with those policies. If the field is flagged as critical, the CA is specifically limiting use of the certificate to situations in accordance with the policies." Version 3 X.509 Certificates, Entrust Technologies White Paper, Section 31. The *certificatePolicies* extension is used to insure that certificate users have an authentic and non-reputable indication of the policy under which the certificate was issued, and hence the applications for which it is suitable. This extension helps to prevent a verifier from using a certificate for a purpose other than that intended by the issuing CA. This also prevents a signer from repudiating a signature on the grounds that he/she did not intend the associated signature to be used for that purpose. Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 4.

[18] Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997 at Section 3.6.

It is clear that a given class of certificates issued by a given certification authority can support (i.e., be issued consistent with) several certificate policies, so long as the certificates satisfy the requirements of all such certificate policies. Likewise, a given certificate policy (such as one that might be adopted by an automobile industry trade association), can be supported by many certification authorities operating under separate certification practice statements.

2. Purpose

A certificate policy can serve a variety of purposes for both certification authorities and relying parties. This Model Policy is written from the perspective of a relying party to fulfill the following primary purposes:

- Requirements Device for Relying Parties -- Through the establishment or endorsement of a certificate policy, a relying party (or group) can specify its requirements for the level of assurance or trust necessary for certificates that will be used in certain types of electronic transactions that it enters into.
- Accreditation device -- Certificate policies can also constitute a basis for accreditation of CA's. That is, accreditation may be determined through compliance with a particular certificate policy.
- Automated Certificate Review -- A certificate policy can be used to promote interoperability between CAs operated by different organizations and to facilitate the automated acceptance of certificates by relying parties -- i.e., a vehicle on which to base common interoperability standards and common assurance criteria within a community, such as on an industry-wide (or possibly more global) basis.
- Compliance Device for CAs -- By asserting that its certificates are issued in accordance with the terms of a certificate policy, a certification authority can indicate to subscribers and relying parties the suitability of its certificates for the purposes of communicating with relying parties who have specified the policy, and compliance with the requirements of such relying parties.
- Define/Limit Use -- A certificate policy can be used to define the scope of acceptable use for the certificate. "For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range."[19] Likewise, a certificate policy can be used as a device to restrict the purposes for which the certificate is intended to be used (e.g., for SET transactions, for access to the ABC Garden Club Web site, for purchase transactions less than $5,000, etc). This helps to prevent a relying party from using a certificate for a purpose other than that intended by the issuing CA.

[19] ITU-T X.509 Recommendation, Section 3.3.

This also prevents a signer from repudiating a signature on the grounds that he/she did not intend the associated signature to be used for that purpose.[20]

- Risk Assessment Device for Relying Parties -- A certificate policy can also be viewed as a risk assessment device for relying parties -- i.e., it is a statement of the practices and procedures involved in the generation, management, and revocation of the certificate that is intended to be used by the relying party to evaluate the strength or trustworthiness of the certificate.

3. Level of Specificity

A certificate policy is a high level document. "A certificate policy represents a limited set of practice provisions . . . a less precise statement of certification practices than a CPS". . .[21] A CPS on the other hand, is "a more detailed description of the practices followed by a CA in issuing and otherwise managing certificates"[22] than that contained in a certificate policy. A CPS implements the general rules imposed by the certificate policies that the CPS supports.

4. Approach

In addition to differing degrees of specificity, the approach of a certificate policy is significantly different than a CPS. A certificate policy is defined independently of the specific details of the operating environment of any particular CA, whereas the corresponding CPS is tailored to the organizational structure, operating procedures, facilities and computing environment of the certification authority.[23] Likewise, a CPS contains a much more comprehensive level of detail "which weds the CPS to a particular (proprietary) implementation of a service offering."[24] Thus, the CPS describes how the certificate policy is interpreted in the context of the system architecture and operating procedures of the CA's organization. In other words, a certificate policy generally states "what" is to be adhered to, while the CPS states "how" it is adhered to.[25] For example:

The following Certificate Policy component:

---

[20] Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 4.

[21] Warwick Ford and Michael S. Baum, Secure Electronic Commerce, (1997) at page 362.

[22] Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997, at Section 1.1. (See also, section 3.6, which notes that CPSs "will generally be more detailed than certificate policy definitions").

[23] Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 2.

[24] Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", PKIX Working Group Internet Draft, September 30, 1997 at Section 3.6.

[25] Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 2.

"Users will inform the Operating Authority immediately upon discovery that their private key has suffered unauthorized disclosure"

may be transformed by an Operating Authority into the following CPS component:

- *"All users (including end-users and operators of CAs) will be informed of the requirement to report unauthorized disclosure of their private key in an agreement, which they will sign prior to their being issued a certificate.*

- *Upon discovery of the unauthorized disclosure of the private key, users will be required to contact their CA, within one working day. The method of contacting the CA will be one of those listed in the CPS.*

- *When not in use, users will be required to keep all copies of their private key either on their person, or in a locked place."*[26]

B. Who Does It Benefit? Who does It Bind?

Implementing the concept of a certificate policy requires consideration of some potentially significant issues relating to the question as to how one becomes entitled to claim the benefits of, and how one becomes obligated by the terms of, a certificate policy. This question applies equally to certification authorities and relying parties.

From the certification authority's perspective, the ability to issue certificates that assert compliance with a particular certificate policy may have marketing benefits. For example, it may be the key to selling certificates to subscribers who need them for communications with a relying party that require certificates issued in compliance with the policy. This raises the question of when, and under what circumstances, a certification authority is entitled to claim that its certificates comply with a particular policy.

Under one model, the ability to claim compliance with a particular certificate policy might be analogous to being able to use a Good Housekeeping seal of approval or an Underwriter's Laboratory certification on one's products. That is, it provides a marketing benefit. Should the issuer of the certificate policy, or some policy administering organization, accredit or certify the practices and procedures of a certification authority before it is entitled to claim the benefit of compliance with the policy? Alternatively, should a claim of compliance be treated simply as in the nature of a representation or warranty by the certification authority that its practices and procedures are in compliance, failing which the CA will be liable for damages?

[26] Example taken from Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0), Section 2.

The flip side of the question is also important. That is, being obligated to the terms of a certificate policy may expose the certification authority to additional liability. Under what circumstances is a certification authority held liable, either in contract or in tort, for damages suffered by a relying party that are the direct and proximate result of the failure of a certification authority to comply with the requirements of a certificate policy? In other words, how does the CA become "bound" to perform in accordance with the certificate policy?

Similar questions also arise with respect to the rights and obligations of relying parties. First and foremost, we must ask who is entitled to claim the benefits of a certificate policy from the perspective of a relying party? Should this be limited to the organization that authors the certificate policy? Or should anyone who declares that they will accept certificates that are issued in compliance with a particular certificate policy be entitled to obtain a legal right against certification authorities who assert compliance with the policy but fail to do so. For that matter, should the benefits of a certificate policy extend to any relying party (regardless of whether they have identified the policy as a requirement), on the theory that an assertion of compliance by a certification authority constitutes something in the nature of a public warranty that can be the basis of a claim by anyone who relied on the warranty and was injured by the failure of the certification authority to perform as represented.

These critical issues will require additional evaluation and debate. The solution will depend, in part, on a legal analysis of the rights and obligations of parties acting in the manner contemplated by a certificate policy. In addition, however, this solution will also depend upon the nature of the business model the parties intend to construct.

The Model Policy set forth in this document is not yet in a position to answer these questions. As to how a certification authority becomes entitled to assert compliance with, and becomes bound by, the certificate policy, the Model proposes two alternatives. Under the first alternative, a certification authority merely asserts or declares its compliance with the policy and begins issuing certificates that reference the policy. By doing so, it is intended that its conduct constitutes an acceptance of the terms of the certificate policy and it is bound thereby. Under the second alternative, a certification authority has to specifically apply to a policy administering organization, enter into an appropriate contract, and successfully complete a compliance audit to establish his compliance with the requirements of the policy.

With respect to relying parties, the Model Policy contemplates that there will be some limited class of parties entitled to rely on the legal benefits of the certificate policy. Tht class of relying parties is referred to as "Qualified Relying Parties" in the Model. However, the exact parameters of that classification are left open and subject to further discussion.

A related question goes to the impact of a certificate policy on the subscriber. To what extent does it, or should it, govern the conduct of the subscriber? It seems doubtful that a certificate policy can specify the rights and obligations of subscribers unless there exists a contract by which the parties so agree. Merely stating so in a certificate policy does not accomplish this

goal. Accordingly, the approach in the Model Policy is to require the CA to enter into an enforceable contract with the subscriber to define the applicable rights and obligations in the specified manner. Alternatively, this problem might be avoided where the Policy is used as system rules applicable to all parties in a given domain.

C. Principles for Certificate Policies

In light of the foregoing, the Model Certificate Policy is drafted to implement the following principles--

- **Perspective.** The Model Certificate Policy is drafted from the perspective of a relying party
- **CA as Responsible Party**. The Model Policy is written under the assumption that the entity defined as the "CA" is responsible for all aspects of the issuance of a certificate, including control over the application/enrollment process, the identification and authentication process, the certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate. The Policy recognizes, however, that certain of these functions may be delegated by the CA to other parties, such as a Registration Authority ("RA"), a Certificate Manufacturing Authority ("CMA"), or a Repository Services Provider ("RSP"). However, the Policy contemplates that the CA remains responsible for the performance of the RA, the CMA, and the RSP, and provides accordingly. Thus, under the Model Policy, there is a single point of responsibility that rests with the CA. While the CA may delegate to others responsibility for accomplishing portions of the required services, the CA remains ultimately responsible for performance of those services by such third parties in a manner consistent with the requirements of the policy.

- **Specificity.** The nature of a certificate policy as a statement of practices potentially applicable to a large number of CAs dictates an approach to writing a certificate policy that is not specific to the details of the system used by any particular CA. Rather, the "set of rules" that comprise the certificate policy must be at a sufficiently high level to state general principles that each CA can further define and implement in the context of its own CPS. The Model Policy avoids the technical and implementation-specific information unique to the way in which each certification authority does business. Those details can be included in each CA's specific CPS.
- **Level of Detail.** The Model Policy is a high-level document specifying "what" principles the CA is to adhere to, not a detailed document stating "how" those principles are to be implemented. Thus, details of specific procedures, such as "how to access the CRL, or how to revoke a certificate" should not be the focus of the Model Policy (e.g., these details can be included in the CPS).
- **Coverage.** In determining what information to include in the Model Policy, the ultimate question is "what does a relying party need to know in order to evaluate the

trustworthiness of the certificate?" Thus, the Model Policy is limited to information relevant for the relying party to determine:

- the suitability of the certificate for the particular application, and
- the level of trust to place in the certificate.

- **Business Models.** The Model Certificate Policy is written to accommodate as many different CA business models as possible (e.g., a traditional CA, a CA operating with a local RA, a virtual CA, a CA that outsources the certificate manufacturing function, etc.).
- **Subscriber Obligations.** The Model Certificate Policy does not purport to create a binding contractual commitment on the subscriber. Instead, it requires the CA to enter into contractual obligations with its subscribers.
- **Key Recovery.** The Model Certificate Policy does not address key recovery or key escrow issues.
- **Open vs. Closed System.** The Model Certificate Policy assumes the CA is working within an open PKI system, but works in a closed system as well.
- **Government and Private CAs.** The Model Certificate Policy covers both government and private CAs.
- **Adaptability.** The Model Certificate Policy is sufficiently generic (e.g., technologically neutral) so that many certification authorities operating under a variety of different CPSs can adopt it (putting technology-specific information into a CPS).
- **Cross Certification.** The current draft of the Model Certificate Policy is limited to certificates issued to end entities (i.e., subscribers), and does not cover cross certification of other CAs. It is expected that future drafts will address this issue.
- **Root Key.** The Model Certificate Policy assumes that the CA is using its own self-signed root key.
- **Focus.** The focus of the Model Certificate Policy is on legal, rather than detailed technical, aspects of the CAs operations.
- **Scope** - Certificates issued under the Model Policy are intended to be suitable for applications requiring a medium level of assurance.
- **Subscribers** -- The subscribers to be certified under the policy may be either independent or associated with a sponsor recognized by the CA.
- **Key Use** -- The policy is intended for use only with certificates containing public keys used for digital signature verification.
- **CA Representations** -- By adopting the Model Policy, a certification authority warrants, represents, and promises to provide certification and repository services consistent with the terms of the Policy.

- **Repository Services** -- CAs that adopt the Policy must directly or indirectly provide repository services. All certificates issued by a CA pursuant to the policy must be published in a public repository maintained by or on behalf of the CA and accessible to all potential relying parties.

- **Direct Damages** -- CAs that adopt the Policy may state a limitation or cap on direct damages. CAs that adopt the Policy may exclude damages that are considered indirect, special, incidental, or consequential, such as loss of profits, loss of data, punitive damages, etc.

- **Disclosure.** CAs using the Model Policy must make publicly available in their repositories all CPS's referencing the Policy, copies of all certificates referencing the Policy, and the CRLs advising of the revocation of any such certificates.

- **Access Controls.** CAs adopting the Model Policy may not impose access controls on the reading of the Policy or its related CPS.

- **Audit** -- CAs operating under the Policy shall be audited at least annually for conformance to the Policy by an independent recognized and credible established audit firm.

D. References and Related Materials

Michael S. Baum, "Federal Certification Authority Liability and Policy," NIST-GCR-94-654 (June 1994).

Sharon Boeyen, "Certificate Policies and Certification Practice Statements", February 1997 (Entrust Technologies White Paper Version 1.0); available at *www.entrust.com*

"Certificate Policies for the Government of Canada Public Key Infrastructure" (Working Draft 10/14/97)

Santosh Chokhani and Warwick Ford, "Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework", September 30, 1997 (PKIX Working Group Internet Draft), available at *www.ietf.org/ids.by.wg/pkix.html*

Warwick Ford and Michael S. Baum, Secure Electronic Commerce Prentice Hall, (1997).

Information Security Committee, Electronic Commerce Division, Section of Science and Technology, American Bar Association, Digital Signature Guidelines (August, 1996); available at *www.abanet.org/ec/isc/dsgfree.html*

International Telecommunications Union, ITU-T Recommendation X.509

S. Kent "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management," Internet RFC 1422, § 3.4 (February, 1993

Thomas J. Smedinghoff, Ed., Online Law (Addison-Wesley, 1996)

Thomas J. Smedinghoff, "Summary of Electronic Commerce and Digital Signature Legislation", available at *www.mbc.com/ds_sum.html*.

II.
MODEL CERTIFICATE POLICY

CONTENTS

MODEL CERTIFICATE POLICY

1. INTRODUCTION

1.1 Overview

This Certificate Policy ("Policy") specifies minimum requirements for the issuance and management of certificates that may be used in verifying digital signatures on the categories of electronic communications specified as suitable applications in Section 1.3.6 of this Policy.

1.2 Policy Identification

This Policy [*is registered with* _____, *and*][27] has been assigned an object identifier (OID) of _____.

1.3 Community & Applicability

1.3.1 Certification Authorities (CAs)[28]

This Policy is binding on each Authorized CA that issues certificates that identify this Policy, and governs its performance with respect to all certificates it issues that reference this Policy. Specific practices and procedures by which the CA implements the requirements of this Policy shall be set forth by the CA in a certification practice statement ("CPS") or other publicly available document, or by contract [with all Qualified Relying Parties].

---

[27] Registration of this Policy is presumably optional, as a CA or a relying party may simply "declare" the Policy.

[28] This Section raises the fundamental question of how a CA becomes authorized to issue certificates that reference this Policy. Two alternatives are presented:

- Under Alternative 1, no "permission" is required. By issuing certificates that reference this Policy, a CA simply decides to comply with (and be bound by) the requirements of this Policy, declares its adherence to the Policy, and begins issuing certificates that reference the Policy. Alternative 1 indicates that issuing a certificate that references this Policy constitutes agreement by the issuing CA to be bound by the terms of the Policy. There is some question as to the enforceability of this approach (since binding a CA to the terms of this Policy by its conduct may require notice of the existence of the Policy, and an opportunity to review it). There is also a question as to the identity of the other party or parties with whom the CA is contracting. These are subjects for further research should this approach be deemed desirable.
- Alternative 2 requires preapproval or authorization by the [*Policy Administering Organization]* and the successful completion of an audit designed to verify that the CA does, in fact, operate in accordance with the provisions of this Policy. This approach may be more appropriate for situations where assurance of compliance (rather than a mere warranty) is deemed critical. For example, there may be concern that undercapitalized or poorly managed CAs might otherwise willingly agree to be bound by the terms of the Policy, but then simply ignore its requirements in practice since there is no financial ability to respond in damages for any breach. This approach of alternate 2 might also be appropriate if it is determined that the Policy should allow CAs to significantly limit or cap their liability for breach.

1.3.1.1 CAs Authorized to Issue Certificates under this Policy

[*Alternate 1*] Any CA may issue certificates that identify this Policy provided that such CA agrees to be bound by, and complies with, the undertakings and representations of this Policy with respect to such certificates. Issuance of a certificate that references this Policy shall constitute agreement by the issuing CA to be bound by the terms of this Policy for all certificates that reference this Policy.

[*Alternate 2*] A CA may issue certificates that identify this Policy only if such CA first qualifies as an Authorized CA by:

(a) entering into an agreement with [*the Policy Administering Organization*], for the benefit of all Qualified Relying Parties,[29] to be bound by, and comply with, the undertakings and representations of this Policy, with respect to the class of certificates that are issued with reference to this Policy, and

(b) being approved by [*the Policy Administering Organization*],[30] following successful completion of the compliance audit specified in Section 2.7, a review of its CPS, and satisfaction of [*other applicable requirements*].

1.3.2 Registration Authorities and Certificate Manufacturing Authorities

See Section 2.1.2.

1.3.3 Repositories

See Section 2.1.2.

1.3.4 Subscribers

A CA may issue certificates that reference this Policy to the following classes of subscribers:

---

[29] In many respects, relying parties are beneficiaries of this Certificate Policy and should be entitled to enforce its provisions against the CA in the event of breach (See section 2.2 below). However, this may be appropriate only for narrowly drawn categories of relying parties, referred to here as Qualified Relying Parties (see Section 1.3.5). From the CA's perspective, there is presumably a concern that a potentially infinite pool of relying parties may create an unacceptable risk. Also, it may be appropriate to consider whether this Certificate Policy should impose obligations on Relying Parties (and if it does, how can it make that enforceable?). One approach is to state obligations of relying parties that are simply preconditions to a right of a relying party to enforce any claim against the CA under this Policy. This would avoid the need to create a binding and enforceable contract between the CA and each relying party.

[30] This section raises the question as to which person or entity should be the one approving a CA's application to issue certificates pursuant to this Policy. For example, if the Policy is issued and maintained by a particular Qualified Relying Party (e.g., a government agency), it may be most appropriate for the relying party that issued the Policy to enter into a contract directly with a CA authorizing the CA to issue certificates in accordance with the Policy. Alternatively, if the Policy is maintained by a separate Policy administering organization (presumably for the benefit of multiple qualified relying parties), it may be more appropriate for the CA to contract with, and be approved by, such Policy administering organization. A third alternative may be to require that the CA be accredited by a specified independent accrediting entity. Ultimately, the question becomes one of determining what is required before a CA can qualify as an "authorized CA".

- individuals (unaffiliated)
- individuals associated with a sponsor recognized by the CA ("affiliated individuals"), provided the sponsor is the subscriber of a valid certificate issued by the CA in accordance with this Policy.
- organizations that qualify as legal entities[31]
- government agencies

1.3.5 Relying Parties

This Policy is intended for the benefit of the following persons who may rely on certificates issued to others that reference this Policy ("Qualified Relying Parties"):[32]

- Federal government agencies that specify this Policy by regulation
- State government agencies that specify this Policy by regulation
- Businesses that __[*contractually agree to this Policy with the Policy Administering Organization/with the CA*]___
- Individuals that _____

1.3.6 Applicability

1.3.6.1 Suitable Applications

In determining the categories of transactions for which certificates issued under this Policy may be used, Federal agencies need to evaluate the relative sensitivity of applications for which they intend to send and receive digitally signed messages, bearing in mind the provisions of the Computer Security Act and applicable regulations relating thereto.

---

[31] This category could include CAs. Is this desirable?

[32] This Section raises the issue of how one obtains the status of a relying party entitled to be benefits of this Policy (a "Qualified Relying Party"), and whether the universe of all Qualified Relying Parties should be limited or defined in a manner so as to provide adequate notice to authorized CAs of their identity. It is important that a person's status as a qualified relying party be clear, so there is no question as to that status. One approach is to limit Qualified Relying Parties to government agencies who specify the Policy by regulation or otherwise, or to private entities that contractually "opt in" to qualified relying party status by virtue of a contract with either the Policy Administering Organization or the authorized CAs. This may be accomplished, for example, through the use of a "system rules" approach such as that currently used in the credit card system or the funds transfer systems. That is, by obtaining and using a credit card, or by engaging in electronic fund transfers, a person commits to be bound by a series of system rules set forth by the issuing credit card company or funds transfer system. This approach also provides a benefit for the authorized CAs, in that the universe of qualified relying parties is somewhat defined, and is bound together by everyone's common adherence to a particular policy or other contractual agreement. It is also important to consider the other possible preconditions that must be satisfied before a person can be considered a "qualified relying party". These could include, for example: (1) mere reliance on certificates issued in accordance with this Policy; (2) where relying parties specify reliance on certificates issued pursuant to the Policy in advance (e.g., by regulation); (3) where relying parties enter into a preexisting contract with the CA wherein the CA agrees to be bound by the terms of the Policy for the benefit of such contracting parties only; or (4) where relying parties enter in to a contract with the Policy Administering Organization to obtain the benefits of the Policy

This section should specify the categories of transactions for which certificates issued under this Policy are considered appropriate. The inclusion of such categories should be based on a qualitative risk analysis whereby agencies should determine the level of identity binding they require for their applications. See Section 3. In making such determinations, agencies should consider the need for low value v. high value certificates, whether applications are critical or non-critical, etc. Examples of language that might be included in this section are set forth in the Appendix.

1.4 Contact Details

This Policy is administered by ("Policy Administering Organization"):[33]

_____

_____

_____

Attn: _____

Phone number: _____

E-mail address: _____

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the application/enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

2.1.1.1 Representations By CA

By issuing a certificate that references this Policy, the CA certifies to the subscriber, and to all Qualified Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS that:

- The CA has issued, and will manage, the certificate in accordance with this Policy

[33] The Policy Administering Organization could be a relying party that developed and issued the Policy (such as a federal government agency, an industry trade association, etc.), or a third party designated as the administering organization by the entity that developed the Policy for the benefit of itself and/or a larger group of qualified relying parties.

- The CA has complied with the requirements of this Policy and its applicable CPS when authenticating the subscriber and issuing the certificate
- There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS
- Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate
- The certificate meets all material requirements of this Policy and the CA's CPS

2.1.2 RA and CMA Obligations

The CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the CA may [delegate/subcontract] performance of these obligations to an identified registration authority ("RA") and/or certificate manufacturing authority ("CMA") provided that the CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy.

2.1.3 Repository Obligations

The CA shall be responsible for providing a repository and performing all associated functions. However, the CA may [delegate/subcontract] performance of this obligation to an identified repository services provider ("RSP"), provided that the CA remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy.

2.1.4 Subscriber Obligations

In all cases, the CA shall require the subscriber to enter into an enforceable contractual commitment [for the benefit of Qualified Relying Parties] obligating the subscriber to:

- generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key
- acknowledge that by accepting the certificate the subscriber is warranting that all information and representations made by the subscriber that are included in the certificate are true
- use the certificate exclusively for authorized and legal purposes, consistent with this Policy
- instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscribers private key

2.1.5 Relying Party Obligations

A Qualified Relying Party has a right to rely on a certificate that references this Policy only if the certificate was used and relied upon for lawful purposes and under circumstances where:

- the reliance was reasonable and in good faith in light of all the circumstances know to the relying party at the time of reliance
- the purpose for which the certificate was used was appropriate under this Policy
- the relying party checked the status of the certificate prior to reliance, or a check of the certificate's status would have indicated that the certificate was valid

2.2 Liability

A CA is responsible to Qualified Relying Parties for direct damages suffered by such relying parties that are caused by the failure of the CA to comply with the terms of this Policy, and sustained by such relying parties as a result of reliance on a certificate in accordance with this Policy, but only to the extent that the damages result from the use of certificates for a suitable applications listed in Section 1.3.6.

[Except as expressly provided in this Policy and in its CPS, CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.]

[The liability of a CA under this Policy shall be limited to direct damages, and shall not exceed _____. CA shall have no liability for consequential damages].

2.3 Financial Responsibility

No stipulation.

2.4 Interpretation & Enforcement

2.4.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the United States and the State of _____

2.4.2 Dispute Resolution Procedures

No stipulation

2.5 Fees

CA shall not impose any fees on the reading of this Policy or its CPS. CA may charge access fees on certificates, certificate status information, or CRLs, subject to agreement between the CA and subscriber, and in accordance with a fee schedule published by the CA in its CPS or otherwise.

2.6 Publication & Repositories

2.6.1 Publication Of CA Information

Each Authorized CA shall operate a secure on-line repository that is available to Qualified Relying Parties and that contains (1) issued certificates that reference this Policy, (2) a Certificate Revocation List ("CRL") or on-line certificate status database, (3) the CA's certificate for its signing key, (4) past and current versions of the CA's CPS, (5) a copy of this Policy, and (6) other relevant information relating to certificates that reference this Policy.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such certificate by the subscriber. Information relating to the revocation of a certificate will be published in accordance with section 4.4.3.

2.6.3 Access Controls

The repository will be available to Qualified Relying Parties [and subscribers] on a substantially 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance and the CA's then current terms of access. CA shall not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the CA's CPS. CA may impose access controls on certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and subscriber, in accordance with provisions published in its CPS or otherwise.

2.7 Compliance Audit[34]

Before initial approval as an Authorized CA, and thereafter at least once every year, the CA (and each RA, CMA, and RSP, as applicable) shall submit to a compliance audit by an independent nationally recognized security audit firm [approved by _____] that is qualified to perform a security audit on a CA and that has significant experience in the application of PKI and cryptographic technologies. The purpose of such audit shall be to verify that the CA has in place a system to assure the quality of the CA Services that it provides, that complies with all of the requirements of this Policy and its CPS, and that its CPS is consistent with the requirements of this Policy.

2.8 Confidentiality Policy

Information regarding subscribers that is submitted on applications for certificates will be kept confidential by CA and shall not be released without the prior consent of the subscriber, unless otherwise required by law. The foregoing shall not apply, however, to information appearing on certificates, or to information regarding subscribers that is obtained by CA from public sources. Under no circumstances shall CA (or any RA, RSP, CMA) have access to the private keys of any subscriber to whom it issues a certificate that references this Policy.

[34] If alternate 1 of Section 1.3.1.1 is used, this section may not be necessary.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

Subject to the requirements noted below, Certificate applications may be communicated from the applicant to the CA or an RA, (and authorizations to issue certificates may be communicated from an RA to the CA), (1) electronically via E-mail or a web site, provided that all communication is secure, such as (1) by using SSL or a similar security protocol, (2) by first class U.S. mail, or (3) in person.

3.1.1 Types of Names

The subject name used for certificate applicants shall be [the *X.509 Distinguished Name*].[35]

3.1.2 Name Meanings

The subject name listed in a certificate must have a reasonable association with the authenticated name of the subscriber. In the case of individuals this should be a combination of first name and/or initials and surname. In the case of an organization the name should reflect the legal name of the organization and/or unit.

3.1.3 Rules For Interpreting Various Name Forms

No stipulation.

3.1.4 Name Uniqueness

The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by the CA. [*and conform to X.500 standards for name uniqueness*]. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the CA.

3.1.5 Verification of Key Pair

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application [*in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol or through other means*].

3.1.6 Authentication of Organization

When a CA receives a certificate application from an organization, it shall conduct an independent investigation in order to determine whether:

- The organization exists and conducts business at the address listed in the certificate application.
- The certificate application was signed by a signatory who was a duly authorized representative of the organization named therein.

[35] Note that there may be other naming constructs that are useful to some communities, and that the technology will support (e.g., rfc822name).

- The information contained in the certificate application is correct.

In conducting its review and investigation, the CA shall review official government records and/or engage the services of a reputable third party vendor of business information to provide validation information concerning each organization applying for a certificate, including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant is incorporated or otherwise organized.

3.1.7 Authentication of Individual -- No Affiliation

In determining the form and type of authentication required for certificates issued pursuant to this Policy, federal agencies should evaluate the relative sensitivity of applications for which they intend to send and receive digitally signed messages. Based on such evaluation, it may be appropriate to authorize on-line identity verification (such as proposed in the ACES program), while in other cases, it may be appropriate to require applicants to personally present themselves, or to provide notarized copies of identity papers. Examples of alternate language that might be included in this section are set forth in the Appendix.

3.1.8 Authentication of Individual – Affiliated Certificate

3.1.8.1 Identification

The CA may establish a trustworthy procedure whereby a sponsoring organization that has been authenticated by the CA and issued a certificate may designate one or more Responsible Individuals, and authorize them to represent the sponsoring organization in connection with the issuance and revocation of certificates for affiliated individuals. The CA may rely on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant (provided that the CA has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with this Policy). In the absence of the foregoing procedure, affiliated individuals shall be authenticated in the same manner as unaffiliated individuals.

3.1.8.2 Authentication Confirmation Procedure

Authentication of the individual will be confirmed through the use of a shared secret [such as a PIN number] that is distributed via a trustworthy out of band communication to the applicant (either directly or via the sponsor) and included in the application process as part of the certificate enrollment process.

3.1.8.3 Personal Presence

Applicants that are affiliated with [an Approved] sponsor can be authenticated through an electronically submitted application, based on an appropriate agreement with the sponsor, the approval of a designated Responsible Individual, and the distribution of PIN numbers or a similar security device.

3.1.8.4 Duties of Responsible Individuals

The Responsible Individual represents the sponsoring organization with respect to the issuance and management of certificates. In that capacity he or she is responsible for properly indicating which subscribers are to receive certificates.

3.2 Renewal Applications (Routine Rekey)

Within _____ months prior to the scheduled expiration of the operational period of a certificate issued following authentication under this Policy, a subscriber may request issuance of a new certificate for a new key pair from the CA that issued the original certificate, provided the original certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original certificate.

3.3 Rekey After Revocation

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate from the CA that reference this Policy shall be re-authenticated by the CA or RA on certificate application, just as with a first-time application.

3.4 Revocation Request

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the old key pair. The identity of a person submitting a revocation request in any other manner shall be authenticated [in accordance with Section ___]. Revocation requests authenticated on the basis of the old (compromised) key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

An applicant for a certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the CA. All applications are subject to review, approval and acceptance by CA. The certificate application process may be initiated by the following persons:

Potential Subscriber	Authorized Initiator
Individual (unaffiliated)	Potential subscriber only
Individual affiliated with a sponsor	Potential subscriber or duly authorized representative of sponsor
Organization	Duly authorized representative of potential subscriber only

4.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the CA shall issue the requested certificate, notify the applicant thereof, and make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially

delivered to, or available for pickup by, the subscriber only. A CA will not issue a certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

4.3 Certificate Acceptance

Following issuance of a certificate, the CA shall contractually require the subscriber to expressly indicate acceptance or rejection of the certificate to the CA, in accordance with procedures established by the CA and specified in the CPS.

4.4 Certificate Revocation

4.4.1 Circumstances For Revocation

4.4.1.1 Permissive Revocation

A subscriber may request revocation of his, her, or its certificate at any time for any reason. A sponsoring organization (where applicable) may request revocation of the certificate of any affiliated individual at any time for any reason. [The issuing CA may also revoke a certificate upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its obligations under this Certificate Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.][36]

4.4.1.2 Required Revocation

A subscriber, or a sponsoring organization (where applicable) shall promptly request revocation of a certificate:

- whenever any of the information on the certificate changes or becomes obsolete
- whenever the private key, or the media holding the private key, associated with the certificate is, or is suspected of having been, compromised
- whenever an affiliated individual is no longer affiliated with the sponsor

The issuing CA shall revoke a certificate:

- upon request of the subscriber or sponsoring organization
- [upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its material obligations under this Certificate Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.][37]
- if knowledge or reasonable suspicion of compromise is obtained
- if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS

In the event that the CA ceases operations, all certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

---

[36] This provision functions much like a "self-help" remedy. In some cases it may be inappropriate to give this authority to the CA in the absence of an appropriate adjudication.

[37] See prior footnote.

4.4.2 Who Can Request Revocation

The only persons permitted to request revocation of a certificate issued pursuant to this Policy are the subscriber, the sponsoring organization (where applicable), and the issuing CA.

4.4.3 Procedure For Revocation Request

A certificate revocation request should be promptly communicated to the issuing CA, either directly or through an RA. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber, or the sponsoring organization (where applicable). Alternatively the subscriber, or sponsoring organization (where applicable), may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

4.4.3.1 Repository/CRL Update

Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CA shall be archived.

4.4.4 Revocation Request Grace Period

Requests for revocation shall be processed within ____ (__) hours/working days of receipt by the CA.

4.4.5 Certificate Suspension

The procedures and requirements stated for certificate revocation must also be followed for certificate suspension where implemented.

4.4.6 CRL Issuance Frequency

When CRLs are used, an up-to-date CRL shall be issued at least every ____ hours.

4.4.7 On-Line Revocation/Status Checking Aavailability

Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated no later than ___ hours after revocation.

4.5 Computer Security Audit Procedures

All significant security events on the CA system should be automatically recorded in audit trail files. The audit log shall be processed at least once a week. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived as per Section 4.6.

4.6 Records Archival

4.6.1 Types Of Records Archived

The following data and files must be archived by [or on behalf of] the CA:

- All computer security audit data

- All certificate application data
- All certificates, and all CRLs or certificate status records generated
- Key histories
- All correspondence between the CA and RAs, CMAs, RSPs, and/or subscribers

4.6.2 Retention Period For Archive

Archive of the key and certificate information must be retained for at least 30 years. Archives of the audit trail files must be retained for at least six (6) months.

4.6.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must be to at least the level required of the _____. It should also be provided adequate protection from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

4.6.5 Archive Collection System (Internal Or External)

No stipulation.

4.6.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives and if either copy is found to be corrupted or damaged in any way it shall be replaced with the other copy held in the separate location.

4.7 Key Changover

No stipulation.

4.8 Compromise And Disaster Recovery

4.8.1 Disaster Recovery Plan

The CA must have in place an appropriate disaster recovery/business resumption plan and must set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy within _____ hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be [detailed/referenced] within the CPS or other appropriate documentation available to Qualified Relying Parties.[38]

[38] Alternatively, it might be appropriate to limit access to this information to the Policy Management Organization.

4.8.2 Key Compromise Plan

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates, or used by any higher level CA. Such plan shall include procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties.

4.9 CA Termination

In the event that the CA ceases operation, all subscribers, sponsoring organizations, RAs, CMAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS[39]

5.1 Physical Security -- Access Controls

The CA, and all RAs, CMAs and RSPs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1. Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of CA (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.2.2 Multiple Roles (Number Of Persons Required Per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CA server should be shared by multiple roles and individuals. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

[39] This section describes the rules and requirements that govern the issuance of a certificate, and the representations made by the CA upon issuance

5.3 Personal Security Controls

5.3.1 Background And Qualifications

CAs, RAs, CMAs, and RSPs shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

5.3.2 Background Investigation

CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

5.3.3 Training Requirements

All CA, RA, CMA, and RSP personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

5.3.4 Documentation Supplied To Personnel

All CA, RA, CMA, and RSP personnel must comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

6. TECHNICAL SECURITY CONTROLS[40]

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

Key pairs for CAs, CMAs, RAs, RSPs, and subscribers must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Acceptable ways of accomplishing this include:

- Having all users (CAs, CMAs, RAs, RSPs, and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else
- Having keys generated in hardware tokens from which the private key cannot be extracted.

CA, RA, and CMA keys must be generated in hardware tokens. Key pairs for RSPs, and end-entities can be generated in either hardware or software.

6.1.2 Private Key Delivery To Entity

See Section 6.1.1.

[40] This section contains provisions of key pair management Policy for CAs, as well as CMAs, RAs, and RSPs (where applicable), and subscribers, and the corresponding technical controls required by those entities.

6.1.3 Subscriber Public Key Delivery To CA

The subscriber's public key must be transferred to the RA or CA in a way that ensures that (1) it has not been changed during transit; (2) the sender possesses the private key that corresponds to the transferred public key; and (3) the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA Public Key Delivery To Users

The public key of the CA signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.

6.1.5 Key Sizes

[*Federal agencies should: (1) define the acceptable algorithms (e.g., RSA signature, DSA,etc.; and (2) specify the minimum key sizes for: CA signing key and user signing key for each algorithm*.]

6.2 CA Private Key Protection

The CA (and the RA, CMA, and RSP) shall each protect its private key(s) in accordance with the provisions of this Policy.

6.2.1 Standards For Cryptographic Module

CA signing key generation, storage and signing operations shall be on a hardware cryptomodule rated at FIPS 140-1 Level 2 (or higher). Subscribers shall use FIPS 140-1 Level 1 approved cryptographic modules (or higher).

6.2.2 Private Key (N-M) Multi-Person Control

No stipulation.

6.2.3 Private Key Escrow

CA signing private keys shall not be escrowed.

6.2.4 Private Key Backup

An entity may optionally back up its own private key.

6.2.5 Private Key Archival

An entity may optionally archive its own private key.

6.2.6 Private Key Entry Into Cryptographic Module

No stipulation.

6.2.7 Method Of Activating Private Key

No stipulation.

6.2.8 Method Of Deactivating Private Key

No stipulation.

6.2.9 Method Of Destroying Private Key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

6.3 Other Aspects Of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Key Replacement

CA key pairs must be replaced at least every _____ years. RA and subscriber key pairs must be replaced not less than every _____ years and a new certificate issued.

6.3.3 Restrictions On CA's Private Key Use

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and, optionally, CRLs.

A private key used by an RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission of the CA.

A private key held by a CMA and used for purposes of manufacturing certificates for the CA is considered the CA’s signing key, is held by the CMA as a fiduciary for the CA, and shall not be used for any reason without the express permission of the CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

All CA servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards: _____.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system design and development shall be conducted using a methodology that _____.

6.6.2 Security Management Controls

6.7 Network Security Controls

The CA server and repository must be protected through application level (proxy) firewalls (or separate ports of a single firewall) configured to allow only the protocols and commands required for the CA’s services.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages -- i.e., public keys used for digital signature verification.

All certificates that reference this Policy will be issued in the [*X.509 version 3*] format and will include a reference to the OID for this Policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extension, [*consistent with the profile developed by the FPKI-TWG]*.

7.2 CRL Profile

If utilized, CRLs will be issued in the [*X.509 version 2*] format. The CPS shall identify the CRL extensions supported and the level of support for these extensions. [*consistent with the profile developed by the FPKI-TWG*]

8. POLICY ADMINISTRATION

8.1 Policy Change Procedures

8.1.1 List Of Items

Notice of all proposed changes to this Policy under consideration by the Policy Administering Organization that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to Authorized CAs, and will be posted on the World Wide Web site of the Policy Administering Organization. Authorized CAs shall post notice of such proposed changes in their repositories and shall advise their subscribers, in writing or by e-mail, of such proposed changes.

8.1.2 Comment Period

Impacted users may file comments with the Policy Administering Organization within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 Publication & Notification Procedures

A copy of this Certificate Policy is available in electronic form on the Internet at _____, and via e-mail from _____. Authorized CAs shall post copies of this Policy in their repositories.

9. DEFINITIONS

Affiliated Individual. An affiliated individual is the subject of a certificate that is affiliated with a sponsor approved by the CA (such as an employee affiliated with an employer).

Certificates issued to affiliated individuals are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

Authorized CA. Means a certification authority that has been authorized by the Policy Administering Organization to issue certificates that reference this policy.

CA. Certification Authority

Certificate. A record that, at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) identifies its operational period; and (e) contains a certificate serial number and is digitally signed by the certification authority issuing it. As used in this Policy, the term of "Certificate" refers to certificates that expressly reference this Policy in the "*certificatePolicies*" field of an X.509 v.3 certificate.

CMA. See Certificate Manufacturing Authority

Certificate Manufacturing Authority" (CMA). An entity that is responsible for the manufacturing and delivery of certificates signed by a certification authority, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is delegated or outsourced the task of actually manufacturing the certificate on behalf of a CA).

Certificate Revocation List (CRL). A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration authority (RA) and a certificate manufacturing authority (CMA), or it can delegate or outsource either of these functions to separate entities.

A certification authority performs two essential functions. First, it is responsible for identifying and authenticating the intended subscriber to be name in a certificate, and verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair.

Certification Practice Statement (CPS). A "certification practice statement" is a statement of the practices that a certification authority employs in issuing, suspending, and revoking certificates and providing access to same.

CMA. See Certificate Manufacturing Authority.

CPS. See Certificate Practices Statement.

CRL. See Certificate Revocation List.

FIPS. Federal Information Processing Standards. These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

IETF. Internet Engineering Task Force. The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Key pair. Means two mathematically related keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

RA. See "Registration Authority."

Object Identifier. An object identifier is a specially-formatted number that is registered with an internationally-recognized standards organization.

OID. See Object Identifier.

Operational Period Of A Certificate. The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

PIN. Personal Identification Number

PKI. Public Key Infrastructure

PKIX. An IETF Working Group developing technical specifications for a PKI components based on X.509 Version 3 certificates.

Policy. Means this Certificate Policy.

Policy Administering Organization. The entity specified in Section 1.4.

Private Key. Means the key of a key pair used to create a digital signature. This key must be kept a secret.

Public Key. Means the key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by a certification authority and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

RA. See Registration Authority.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party. A recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

Repository. A trustworthy system for storing and retrieving certificates and other information relating to those certificates.

Repository Services Provider (RSP). An entity that maintains a repository accessible to the public [or at least to relying parties] for purposes of obtaining copies of certificates and/or verifying the status of such certificates.

Responsible Individual. A person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke A Certificate. Means to prematurely end the operational period of a certificate from a specified time forward.

RSP. See Repository Services Provider.

Sponsor. An organization with which a subscriber is affiliated (e.g., as an employee, user of a service, business partner customer etc.).

Subject. A person whose public key is certified in a certificate. Also referred to as a "subscriber".

Subscriber. A subscriber is a person who (1) is the subject named or identified in a certificate issued to such person and (2) holds a private key that corresponds to a public key listed

in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a certificate. Means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate. Means a certificate that (1) a certification authority has issued, (2) the subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by a certification authority and has been accepted by the subscriber.

APPENDIX

Sample Provisions

1.3.6 Applicability

1.3.6.1 Suitable Applications

Certificates that reference this Policy are intended to provide a medium level of assurance of identity binding, and are typically suitable for:

- verifying the identity of electronic mail correspondents for non-critical communications
- transactions for goods or services of value up to $_____.
- obtaining personal data relating to the subscriber
- obtaining access to [confidential] on-line data bases
- communications between government agencies that are subject to FOIA disclosure

1.3.6.2 Approved Applications

Certificates that reference this Policy may be used for any purpose authorized by regulations adopted by Qualified Relying Parties, except to the extent specifically prohibited by the CA's CPS.

1.3.6.3 Prohibited Applications

Certificates that reference this Policy may not be used for the following applications:

- transactions where the value exceeds $_____
- classified/confidential communications between government agencies
- any application requiring fail-safe performance such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or environmental damage.
- _____

1.3.6 Applicability

1.3.6.1 Suitable Applications

Certificates that reference this Policy are intended to support verification of digital signatures in applications where the identity of communicating parties needs to be authenticated, where a message or file needs to be bound to the identity of its originator by a signature, and/or where the integrity of the file or message has to be assured.

Sample applications this Policy would be suitable for are:

- Applications providing access to the certificate holder's own personal information
- Request and distribution of text information or other types of copyrighted content for which fees are charged or subscriptions are required.
- Verifying the identity of communicating parties.
- Verifying signatures on low and moderate value contracts, Government benefits statements and other documentation.
- Signing of electronic messages.

3.1.9 Authentication of individual -- No Affiliation

3.1.9.1 Identification

In authenticating an unaffiliated individual applicant, the CA or RA shall require two pieces of identification. At least one piece of identification shall be a federal or state government-issued picture-type identification such as a military or government identification card, drivers license, or a passport. Copies of the identification used to establish the subscriber's identity shall be initialed by the CA or RA upon acceptance and archived.

3.1.9.2 Investigation And Confirmation

No Stipulation

3.1.9.3 Personal Presence

Authentication of an unaffiliated individual requires that the applicant must either (1) personally present himself or herself to a CA or RA to be authenticated prior to certificate issuance, or (2) securely deliver signed and notarized copies of the requisite identification to the CA or the RA [in which case, electronic procedures may be used thereafter]. Where the applicant delivers notarized copies of identification to the CA or RA, authentication of such identification will be confirmed through the use of a shared secret [such as a PIN number] that is separately communicated in a trustworthy manner to the applicant and included with the documents delivered as part of the certificate application process.

3.1.9 Authentication of individual -- No Affiliation

3.1.9.1 Identification

In authenticating an unaffiliated individual applicant, the CA or RA shall require the following data elements, which may be submitted electronically:

- Last name (family name)
- First name (given name)
- Middle name(s)
- Street address (no P.O. Boxes)
- City
- State
- Zip
- Social Security Number (SSN)
- Driver's license #, or state identification card #
- Date of birth
- Place of birth
- Telephone number (optional)
- E-mail address (optional)
- Post data element (e.g. mother's maiden name, password, etc.) to be used at a later date for authenticating an individual in the absence of their digital signature; this element could be used along with additional information to authenticate a request for certificate revocations.

3.1.9.2 Investigation And Confirmation

Verification of the Name and SSN and the Name and Driver's License (or ID Number) data elements may be accomplished via online checks with the Social Security Administration and the appropriate state motor vehicle administration respectively. Verification of the Name and Address data elements may be accomplished through access to either a trusted commercial or governmental data source. The address confirmation data sources could consist of either online databases (e.g. Experian or Equifax) or local business records (e.g., a bank's customer records, the U.S. Postal Service, a state motor vehicle office, etc.).

3.1.9.3 Personal Presence

If a CA elected to use an online commercial database, the application may be filled out and submitted via the Internet from a home or business computer. In the case where a CA elects to use a local record check, the application process may take place over the Internet, or alternatively, the CA may require that the applicant visit an appropriate business site in order to enter the required information at a local terminal.